



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,074	03/26/2001	W. Dale Hopkins	20206-15 (P00-3323)	9764
7590	12/20/2005		EXAMINER	
Hewlett-Packard Company Attn. Bill Streeter Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			NALVEN, ANDREW L	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 12/20/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

**Supplemental
Notice of Allowability**

Application No.

09/818,074

Examiner

Andrew L. Nalven

Applicant(s)

HOPKINS ET AL.

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment submitted 4/12/2005.
2. ☒ The allowed claim(s) is/are 1-3,5-18,20,22-51 and 53.
3. ☒ The drawings filed on 3/26/2001 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jonathon Harris (reg# 44,144) on 15 December 2005.

The application has been amended as follows:

Claim 5. A method as recited in claim 1 wherein:

said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including an associated public key exponent value e ;

and said step of receiving includes receiving a request specifying characteristics further including a specified public key exponent value.

Claim 8. A method as recited in claim 1 wherein said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including at least one set of Chinese Remainder Algorithm coefficients pre-computed based on said k associated prime number values prime number values $p_1, p_2, \dots p_k$; and

said step of receiving includes receiving a request specifying characteristics further including a specified type of Chinese Remainder Algorithm.

Allowable Subject Matter

1. Claims 1-3, 5-18, 20, 22-51, and 53 are allowed.

The following is an examiner's statement of reasons for allowance:

2. The reasons for indicating allowable subject matter can be found in the office actions dated 3/16/2005 and 9/9/2004. With regards to claims 43, the provided subject matter presents limitations directed to a series of modules for processing cryptographic transactions. It is clear from the preamble that the modules are embodied within a computing system and thus the claim is not directed towards a purely software implemented system.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

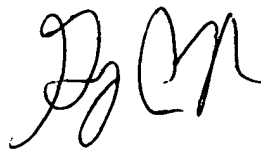
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



GREGORY MORSE
SUPERVISOR
ART UNIT 2134
COMMUNICATIONS SECTION
AUG 16 2009